ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 10, October 2017

Secret Communication over Audio for Defense Application

[1] Parthipan.V , [2] Pakyala.Vidhya
[1]UG student, Department of Computer Science & Engineering, Saveetha University, Chennai, India.
[2]Associate Professor, Department of Computer Science & Engineering, Saveetha University, Chennai, India.

Abstract: ***A steganographic method of embedding textual facts in an audio document is provided in this paper. within the proposed method, first the audio document is sampled and then the appropriate bit of each exchange sample is altered to embed the textual data. As it approach the perceptual great of the host audio sign changed into now not to be degraded.It is a specialty of sending shrouded information or mystery messages over an open channel so that an outsider can't identify the nearness of the mystery messages. The objective of steganography is not the same as traditional encryption, which looks to cover the substance of mystery messages; steganography is about concealing the very presence of the mystery messages. Advanced steganography is for the most part comprehended to manage electronic media as opposed to physical items. There have been various proposition for conventions to shroud information in channels containing pictures, video, sound and even typeset content. This bodes well for various reasons. As a matter of first importance, in light of the fact that the measure of the data is by and large entirely little contrasted with the span of the information in which it must be concealed (the spread content), electronic media is much less demanding to control keeping in mind the end goal to shroud information and concentrate messages. Besides, extraction itself can be mechanized when the information is electronic, since PCs can proficiently control the information and execute the calculations important to recover the messages. Electronic information additionally frequently incorporates excess, superfluous and unnoticed information spaces which can be controlled keeping in mind the end goal to shroud messages.***

I. INTRODUCTION

In these days's global the artwork of sending & displaying the Hidden records particularly in public locations has obtained extra attention and faced many demanding situations. therefore, distinct techniques were proposed so far for hiding information in one-of-a-kind cowl media. on this paper a technique for hiding of facts at the billboard show is offered. it's miles widely recognized that encryption provides relaxed channels for speaking entities. but, due to loss of covertness on those channels, an eavesdropper can identify encrypted streams through statistical exams and seize them for in addition cryptanalysis. in this paper we advocate a new shape of Steganography. Steganography is an artwork of sending hidden records or mystery messages over a public channel in order that a third birthday celebration cannot come across the presence of the secret messages. The aim of Steganography isn't like classical encryption, which seeks to conceal the content of secret messages; Steganography is about hiding the very existence of the name of the game messages. modern Steganography is normally understood to address electronic media in preference to bodily items. There have been numerous proposals for protocols to hide records in channels containing pictures [1, 2, 3], video [3, 4], audio [1, 3] and even typeset textual content [1, 3]. This makes experience for some of reasons. First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and extractmessages. Secondly, extraction itself may be computerized while the statistics is electronic, on account that computers can correctly manipulate the statistics and execute the algorithms important to retrieve the messages. electronic facts also regularly includes redundant, unnecessary and left out facts areas which can be manipulated a good way to hide messages. the primary aim of this paper changed into to discover a manner so that an audio file may be used as a host media to cover textual message without affecting the record structure and content material of the audio record. due to the fact degradation inside the perceptual quality of the quilt item may results in a sizeable change within the cowl object which may additionally ends in the failure of goal of Steganography.

II. PROPOSED METHOD

A. LSB based totally Audio Steganography:

• within the modern-day enterprise, an audio report with ".wav" extension has been selected as host document. it is assumed that the least

• considerable bits of that file should be changed with out degrading the sound first-rate.

B. benefits of Proposed method:

• Secrecy - The embedding mystery text is thought to the sender and the receiver only.

• Imperceptibility – The medium after being embedded with the covert statistics is indiscernible from the original medium. One can't come to be suspicious of the lifestyles of the covert information inside the medium.

• excessive ability - The maximum length of the covert message that can be embedded so long as viable depending on the dimensions of the covering medium (audio).

Applications:

3. Secured Data Transmission
4. Military Applications

Embedding:

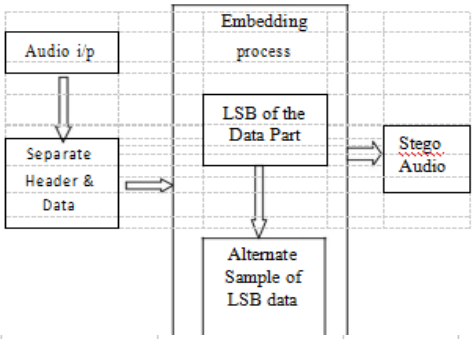

Fig .1 Embedding process

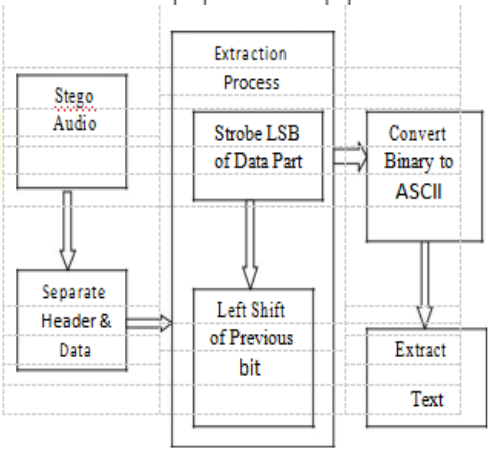

Fig.2 Extraction process

III. RELATED WORKS:

A survey of steganographic techniques exhibits that there had been numerous techniques for hiding statistics or messages in host messages in such a manner that the embedded information ought to be imperceptible. Substitution system substitutes redundant components of a cowl with a secret message. spread spectrum strategies undertake thoughts from spread spectrum conversation. The statistical technique encodes statistics via converting numerous statistical homes of a cowl and use hypothesis checking out in the extraction system. Distortion manner shops information through signal distortion and measure the ccover era method encodes information in the way a cover for secret conversation is created. In case of hiding facts in digital sound, phase Coding embeds information through altering the section in a predefined way. To a certain volume, changes of the section of a sign can not be perceived through the human auditory device (HAS) .these types of steganographic techniques address some not unusual kinds of steganography process relying on the variant of the host media. which means the quilt item or the carrier object so that it will be used to hide the name of the game information. special media like photograph, text, video and audio has been used as a carrier or host media in one of a kind instances. the use of audio document as a cover object directs to Audio steganography. practical audio embedding systems face difficult demanding situations in enjoyable all 3 necessities because of the large electricity and dynamic variety of listening to, and the

huge variety of audible frequency of the. The human auditory machine (HAS) perceives sounds over a range of electricity greater than 109:1 and a number frequencies more than 103:1. The sensitivity of the HAS to the Additive White Gaussian Noise (AWGN) is high as properly; this noise in a valid file may be detected as little as 70 dB below ambient degree. then again, contrary to its big dynamic variety, HAS incorporates a reasonably small differential variety, i.e. loud sounds typically tend to masks out weaker sounds . additionally, HAS is insensitive to a regular relative phase shift in a stationary audio signal and a few spectral distortions interprets as herbal, perceptually non -disturbing ones. two homes of the HAS dominantly utilized in steganographic strategies are frequency masking and temporal masking. The concept using the perceptual holes of the HAS is taken from wideband audio coding (e.g. MPEG compression 1, layer three, normally called mp3) . in the compression algorithms , the holes are used on the way to lower the quantity of the bits needed to encode audio signal, with out causing a perceptual distortion to the coded audio. then again, within the records hiding situations, overlaying houses are used to embed additional bits into an current bit movement, again without generating audible noise in the audio collection used for statistics hiding. some of the audio steganographic strategies are Lossless Adaptive virtual Audio Steganography, LSB based Audio Steganography, Audio Steganography using bit change and so on.

IV. DESIGN METHODOLOGY:

In the modern enterprise, an audio document with ".wav" extension has been decided on as host record. it's miles assumed that the least tremendous bits of that report need to be changed with out degrading the sound exceptional. To try this, first one needs to know the record structure of the audio report. Like maximum files,WAV documents have two basic components, the header and the information. In ordinary wav files, the header is located within the first forty four bytes of the record. except the primary forty four bytes, the rest of the bytes of the report are all about the data. The facts is just one massive bite of samples that represents the complete audio. at the same time as embedding facts, you can actually't cope with the header section. this is due to the fact a minimal trade within the header section leads to a corrupted audio report. A application has been evolved which could read the audio record little by little and stores them in a specific document. the primary 44 bytes should be left with none change in them due to the fact these are the facts of the header phase. Then begin with the ultimate statistics discipline to adjust them to embed textual statistics. for example, if the phrase "Audio" must be embedded into an audio record one has to embed the binary values of the phrase "Audio" into the audio facts discipline. Consider the following table:

Table I- Letters with ASCII and Corresponding Binary Values

Letter	ASCII Value	Corresponding Binary Value
A	65	1000001
u	117	1110101
d	100	1100100
i	105	1101001
o	111	1101111

From the table, you could come to a point that to embed the word "Audio" into the host audio report surely the corresponding 8 bit binary values need to be embedded into the statistics field of that audio file.

V. ALGORITHM:

To develop this algorithm multiple bits of each sample of the file have been changed or modified to insert text data in it. It has also been observed the degradation of the host audio file after modification of the bits. The bit modification was done by various ways, like 1, 2, 3, 4 bits were changed in turn. But after going through all the modification it has been observed that 1 bit change in LSB gave the best result. Thus, data can be embedded according to the following algorithm.

A. Algorithm (For Embedding of Data):

• depart the header phase of the audio document untouched...

• start from a suitable position of the data bytes. (For the experiment purpose the prevailing begin byte became the 51st byte). Edit the least sizable bit with the records that must be embedded.

• Take each alternate pattern and alternate the least widespread bit to embed the entire message. The records retrieving set of rules on the receiver's quit follows the same logic because the embedding set of rules.

B. Algorithm (For Extracting of Data):

• depart first 50 bytes.
• start from the 51st byte and shop the least extensive bit in a queue.
• check every trade sample and keep the least considerable bit within the preceding queue with a left shift of the preceding bit.
• Convert the binary values to decimal to get the ASCII values of the name of the game message.
5. From the ASCII locate the name of the game message.

VI. EXPERIMENTATION, RESULTS AND INTERPRETATION:

An audio report named "audio.wav" has been decided on for this experiment. After checking the binary values of every sample, first 44 samples had been left without any adjustments. The data embedding with LSB modification has been started after the header section. If the records embedding system is commenced from 51st sample then the LSB value of the 51st sample need to be modified. If the binary fee of the corresponding sample is "01110100" then "1" should be modified. From table I it may be determined that to embed the letter "A", the sender has to embed the binary cost "01000001". this is why in step with the embedding set of rules "A" must be embedded in keeping with table II.

TABLE II
SAMPLES OF AUDIO FILES BINARY VALUES BEFORE AND AFTER EMBEDDING

Sample no.	Binary values corresponding sample	Binary value to be embedded	Binary values after modification
51	01110100	0	01110100
53	01011111	1	01011111
55	10001010	0	10001010
57	01111010	0	01111010
59	10100010	0	10100010
61	00110010	0	00110010
63	11101110	0	11101110
65	1011100	1	1011101

in line with the equal way the final consecutive letters of the phrase "Audio" is embedded within the file "audio.wav." editing of the present binary values with the intended binary values reasons a minimal trade inside the audio document "audio.wav" that stays almost imperceptible to all and sundry other than the sender.on the subject of the point of facts retrieving on the Receiver's end, the retrieving algorithm must be followed:

First, exchange the audio message into binary format that has come from the supply as stego-item. leave first 50 bytes and not using a change in them. start from 51st bit, check the least widespread bit, and keep it in a queue. Check every exchange pattern to acquire the entire messages. Like 53rd, 55th and 57th and so forth. save the least big bits of the change samples within the queue with left shift of preceding bit. Convert the binary values to decimal to get back the ASCII from which the textual content may be retrieved. The complete retrieval technique may be depicted with the following desk greater thoroughly:

TABLE III
EXTRACTION OF DATA FROM AUDIO FILE

Sample no	Binary values with embedded secret data	Bits that are stored in the queue
51	01110100	0
53	01011111	01
55	10001010	101
57	01111010	0100
59	10100010	01000
61	00110010	010000
63	11101110	0100000
65	01011101	01000001

As in table II the embedding system of the letter “A” became stated this is why, in desk III, the retrieval method of “A” is depicted. beginning from the 51st pattern, every alternate sample has been checked and the least great bit has been stored into a queue with a left shift of previous bit. after getting all of the bits inside the queue, begin from the left hand aspect, take 8 bits and convert them into equivalent decimal to get the ASCII, from the ASCII retrieve the embedded textual message. From the table, it is absolutely found that upon getting 01000001 in the queue it is transformed into the equal decimal this is sixty five, the ASCII of “A”. as a result “A” is retrieved. just like the identical manner, the next letters also were retrieved and for this reason the entire word “Audio.”

VII. CONCLUSION:

A method of embedding text-based totally facts into a number audio report the usage of the technique of bit modification has been supplied in this paper. A system has been evolved in which the facts subject is edited to embed supposed records into the audio record. To continue with this, the header section of the audio has been checked flawlessly due to the fact a minimum exchange in the header section may also leads to a corruption of whole audio document. in this set of rules, as an test first 50 bytes had been left untouched and beginning from the 51st bytes every trade sample has been changed to embed textual information.How the performance is laid low with converting different bit fields has now not been stated in this paintings. but a rough observe become made to see how the converting of a specific bit field creates degradation in the host audio report and in which factor it results in perceptible exchange in the audible sound high-quality to another third party aside from the sender or receiver. It became noticed that changing the least enormous bit of the bytes gave the high-quality results.

An audio record with length 952 KB has been used. The most textual content record size that may be embedded in this audio report without degrading the file structure may be traced through a survey.

The primary goal of this studies work was embedding of text into audio as a case of steganography. the 2 primary criteria for a hit steganography are that the stego sign attributable to embedding is perceptually indistinguishable from the host audio signal, and the embedded message is recovered efficiently at the receiver. In test instances the text-based facts has been efficaciously embedded to the audio document to visualise in what quantity the target has been completed. however future scope seems countless.

REFERENCES:

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.
[2] Kharrazi, M., Sencar, Husrev T., and Memon, N., “Image Steganography: Concepts and Practice”, WSPC, April 22, 2004.
[3] Stefan Katzenbeisser, Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”. Boston,Artech House, pp. 43 – 82. 2000.
[4] K. Matsui and K. Tanaka. Video-steganography. In: IMA Intellectual Property Project Proceedings, volume 1, pp 187-206, 1994.
[5] N.F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen,” Computer, vol. 31, no. 2, pp. 26-34, IEEE, Feb. 1998.

[6] Matsuoka, H., "Spread Spectrum Audio Steganography using Sub – band Phase Shifting", Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP'06), IEEE, 2006.

[1] S.S. Agaian, D. Akopian, O. Caglayan, S. A. D'Souza, "Lossless Adaptive Digital Audio Steganography," In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903-906, November 2005.

[2] K. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2003.

[9] Mohammad Pooyan, Ahmed Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", International Symposium on Signal Processing and Information Technology, IEEE, 2007.